



# Analysis the importance of VPN for Creating a Safe Connection Over the World of Internet

Md. Zihadul Islam<sup>1</sup>, Mohammad Arifin Rahman Khan<sup>2</sup>, Md. Ibrahim Hossain<sup>3</sup>, Rabbi Hossain<sup>4</sup>

Student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh<sup>1</sup>

Lecturer (Principal Supervisor), Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh<sup>2</sup>

Assistant Professor, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh<sup>3</sup>

Student, Computer Science and Engineering, Bangladesh University, Dhaka, Bangladesh<sup>4</sup>

**Abstract:** Network protection turns into a primary attention of the current period. Each and every sector has benefited from the positive activities of internet, i.e., emergency treatment getting at the current emergency time COVID-19, easily buying and selling the product via the sector of E-Commerce, Digital Research and Education system provide etc. In this manner, the network of communication necessitates the security of the secret information i.e., emergency message, phone calls, medical treatment and report etc. put away or move over the world of internet. Because of the speedy advancement in the area of communication technology and their huge involvement with the task of internet made uncertainty client information, and it also creates the security and protection dangers for the area of medical, business, research, emergency force (i.e., police, army) etc. According to this paper, it is presented that a Virtual Private Network is a good technique for safe the communication instruments and the important information/data from the hacker attacks. A Virtual Private Network (VPN) is a modern technology for a private network that runs on a public network and is used to transmit encrypted information so that attackers cannot able to usage it. The motivation behind Virtual Private Network is to give the specific safety components i.e., realness, classification and information trustworthiness that is the reason these are becoming popular, low-estimated and simple to utilize. The administrations of Virtual Private Network are accessible for advanced mobile phones i.e., smartphones, PCs (Personal Computers), laptops etc. This article focuses too on VPN development, tunnels, security, and protocols. The technique of VPN's activities is a growing generation that performs a main position in Wireless Local Area Network (WLAN) with the aid of using offering steady records transmission over the world of internet.

## I. INTRODUCTION

VPN depicts the chance to set up an ensured network association when utilizing public networks. This network permits are the arrangement of private network facilities for an association on a public communication network like the facility of Internet i.e., fig.1.

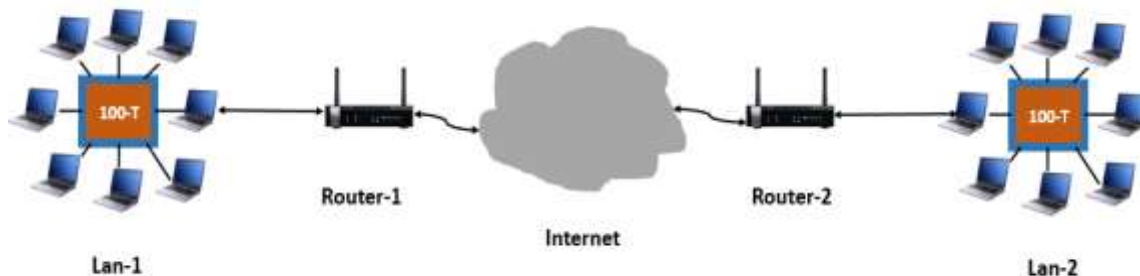


Fig. 1: The network scenario following the internet by the use of VPN.

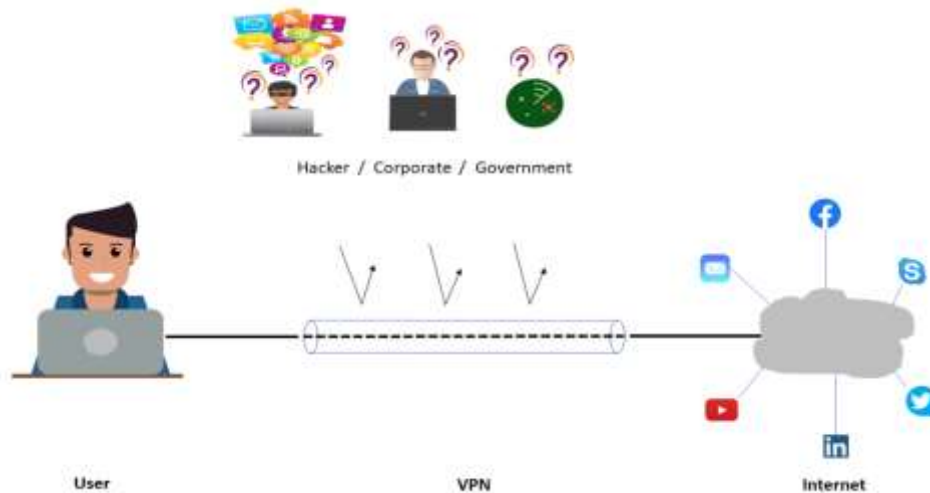
VPN reduces the cost of remote access by using public network resources. VPNs lessen far off get entry to charges through the use of public network resources. Compared to different solutions, together with non-public networks, a VPN is inexpensive [1]. At the current situation for the communication sector Virtual Private Network (VPN) are one of the important technologies and also most steady piece of any kind of IT business since it protects the immense expense of substructure via applying the open Internet to make profoundly shielded the medium of communication from the corporate office to secluded destinations and clients.



## II. BACKGROUND AND LITERATURE REVIEW

Almost 15 years earlier, access from VPN was use for taking another idea to most of the business sector. That starting point can be seen under the area of Virtual Circuit [2]. That administration is viewed as better than an association less help for dealing with long messages. The infrastructure of the VC (Virtual Circuit) is to make a logical direction from the supply one port to another port of the destination. This direction can also additionally combine several hops among routers/switches for the arrangement of the circuit. The concluding, logical direction or the acts of the digital circuit withinside the equal manner as an instantaneous connection among the 2 ports. According to this manner, at least 2 applications could convey over a common communication network. The technology of VC forges in advance by the adjacent of encryption centres to the systems of router. This novel facility begins changing information into a code to save the data from illegal access. Thereafter, different apparatuses had been added as tokens confirmation. Critically, communication lines are still insecure, which has led to the development of protected communication through open networks VPN.

Commonly, Virtual Private Network is a subscriptions-primarily based totally model. This means that users must download the application from their provider and register within a specified period of time to practice their private network to defend dissimilar devices. Prices will vary among providers however normally; that is a regularly scheduled instalment that will consistently diminish dependent on the time length of the membership time frame (month to month or yearly). Free VPN applications for various operating systems are also obtainable in the Store of App [3]. Before the usage of VPN, please keep in mind that your VPN provider may save records of the user's online events, and if they ask, these records are likely to be shared with the authorities.



**Fig. 2: The complete working procedure using VPN.**

According to the buyer's perspective, the significant advantages of Virtual Private Networks are that they are significantly reasonable price [4]. The strategy to the usage of VPN technology is the excessive pace leased line. Those lines are not in cost-effective, hard to control and also tough to maintain. The system of internet gives reliability for the operators of VPN, and not only that it also helps to provides from a very faraway places is to connection to the net the use of dial-up modems. VPNs ensure to provide a safe communication of network for dial in clients (fig.2). The internet gives the Virtual Private Network to the precision of administrations. Mobile clients will most likely be unable to utilize rented lines to associate by the corporate site thus the main conceivable solution is the modern technology of VPN. Moreover, the importance for the use of VPNs are i.e., Shields from cybercriminals [5], Information move is encoded, Territorial rented lines or even link (i.e., cable) networks are all the user need to associate with the net connection and utilize the public community to tunnel a non-public connection for definite, VPN helps to avoid the throttling of data and also prevent the throttling of bandwidth [6], and It also helps to provide the network scalability, reduce the amount of support cost, more secure data transfer.

## III. METHODOLOGY

This topic was chosen to be more familiar in theory in the field of secure network connections using VPNs. In order to complete this project, I did the following things:

- 1). Various articles withinside the Internet have been very well tested and records turned into collected.
- 2). Several e-books and books from the library have been used to discover the content material approximately the topics.
- 3). Consultation with the principal supervisor and the project team was also done which helped in conduction the research



in more depth.

4.) For realistic test, I have experienced www.vpnforuk.com for checking out free VPN service.

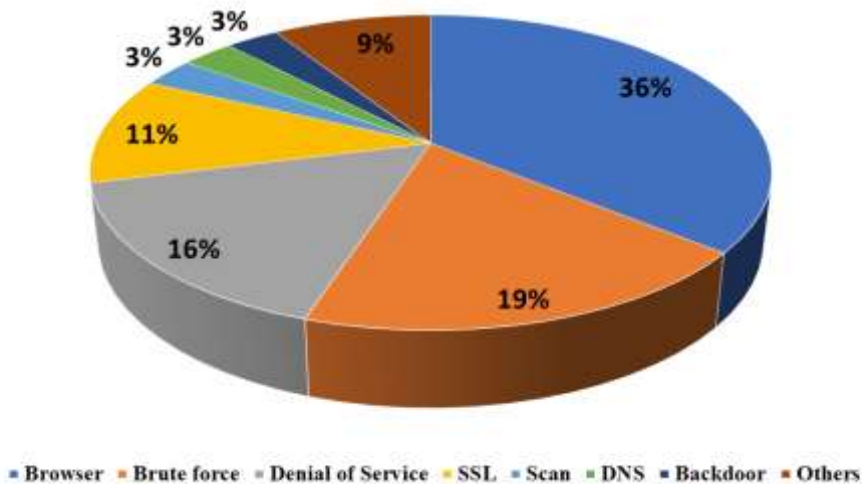
5.) Practical implement the scenario of network using VPN has established in Bangladesh University.

**IV. STUDY FOR THE NEEDS OF SECURITY OVER THE WORLD OF INTERNET**

According to the statistics report from McAfee Labs, 2016 (fig. 3), it has been shown clearly to us that the online system has been affected by unauthorized activities, which makes it possible for a breakdown of the total system of the network and it causes the situation of data plunder by the hackers.

The World of Internet attacked by the unauthorized activities in the year of 2016

Source: McAfee Labs, 2016

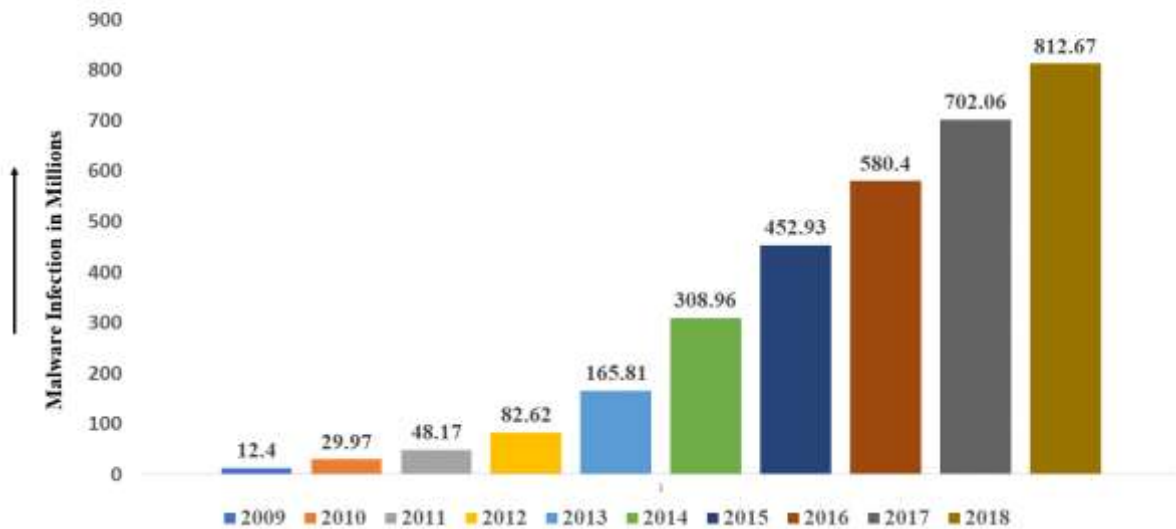


**Fig. 3: The World of Internet attacked by the unauthorized activities, (Source: McAfee Lab, 2016).**

Moreover, according to a report from the year of 2009 to 2018 for the Malware attack on the world of internet users (fig. 4), it can clearly say that network systems, email, emergency data etc. will be in danger and may happen to be destroyed or theft by the hackers.

The Growth Rate of Malware attacked between the year of 2009 to 2018.

Source: PurpleSec LLC, United States.



**Fig. 4: The online users attacked by the Malware, (Source: PurpleSec LLC, United States).**



According to the fig. 3 and figs. 4, it has to find clearly that, the security for the online user is urgency in the future, and this is an extremely headache for all kinds of expert that, how this security will make ensure for the future internet user, and there may have a good solution for the milestone technology of Virtual Private Network.

## V. ANALYSIS THE TOTAL PERFORMANCE OF VPN, AND SECURITY METHODOLOGY

### STRUCTURE OF VIRTUAL PRIVATE NETWORK (VPN):

**Tunnel:** The modern technology of VPN primarily based totally at the idea of tunnelling [9]. The concept of tunnelling for VPN includes setting up and retaining connection of logical network (which could incorporate intermediate hops). According to this connection, packets built in a particular the layout of VPN protocol are encapsulated inside a number of dissimilar base or provider protocol, and after transmitted between the VPN consumer and the server, and in the end de-encapsulated at the reception side. VPN helps forms of tunnelling-voluntary and compulsory. Both forms of tunnelling are usually used.

**Remote Access Virtual Private Network:** The technique of VPN for Remote Access is likewise referred to as VPDNs. This are client-to-LAN associates used whilst personnel of an organization and this organization are in faraway off places need to communicate with the organization's personal network. An organization that desires to set up a remote-access VPN as a rule moves to an ESP whose full abbreviation is enterprise service provider. The ESP sets up a NAS (Network access server) network access server and furthermore gives distant clients the product they need for their PC's (fig. 5). Then, according to this point, clients mostly dial the NAS using a complementary number and access the network through their VPN customer Software. VPNs propose a decent outsider client for encrypted, protected connnotations between distant clients inside a private network.

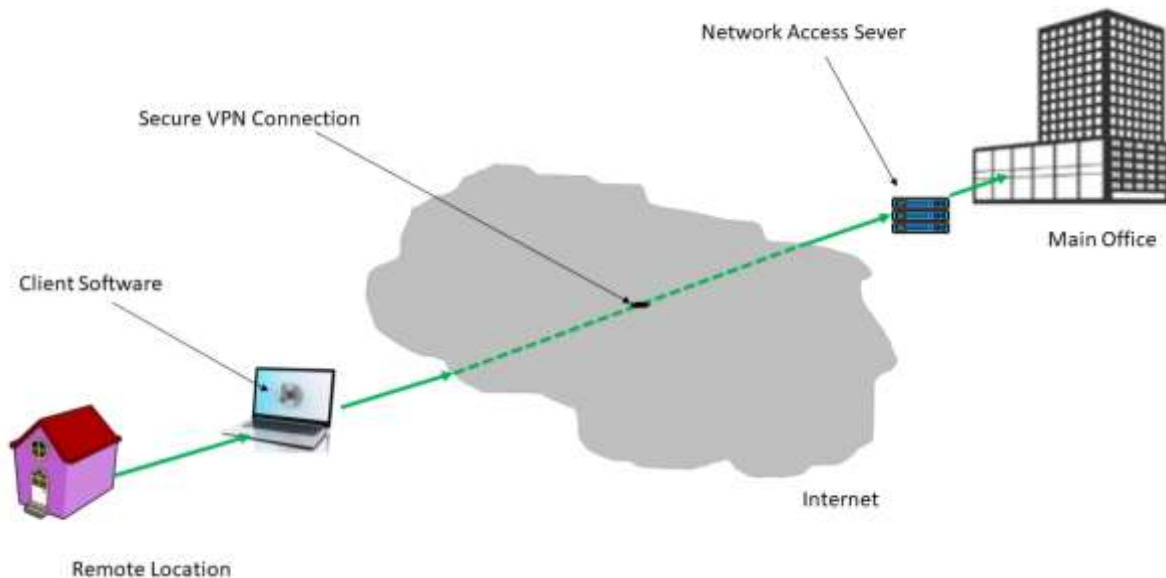
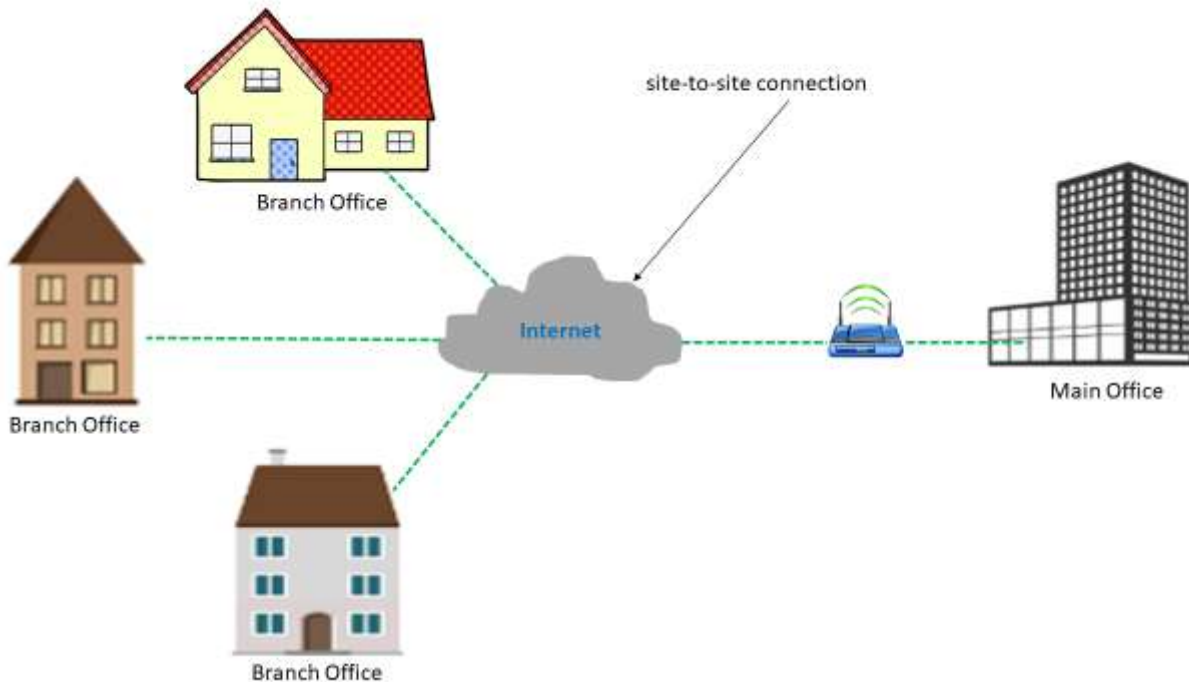


Fig. 5: Available Network scenario for the technique of Remote Access in Virtual Private Network (VPN).

**Site-to-Site Virtual Private Network:** According to the technique of site-to-site Virtual Private Network (VPN) permits workplaces in dissimilar fixed zones to set up protected associations by one another over a public organization [9] i.e., the Internet (fig. 6). This technique for the VPN broadens the network of the company, making the available resources of the computer from one zone accessible to employees at dissimilar zones. An illustration of an organization that needs a site-to-site Virtual Private Network is a developing enterprise through many branches' workplace (i.e., office, factory etc.) all throughout the world.

Normally, two types of site-to-site techniques for VPN are used i.e., intranet based, and Extranet based. According to the technique for intranet based, it can say that, In the event of an organization has minimum one far off zones that they request to link in a single private network, they can make an intranet Virtual Private Network (VPN) to interface each dissimilar Local Area Network (LAN) to a single Wide Area Network (WAN). On the other hand, according to the technique of external based, it can say that in the event of an organization has a near association with additional organization (for example an accomplice, provider, customer etc.), it can assemble an extranet Virtual Private Network that interfaces those organizations' Local area Networks. This site-to-site technique for Virtual Private Network permits the organizations to cooperate in a harmless, shared the resource of network whereas forestalling admittance to their dissimilar intranets.



**Fig. 6: Available Network scenario for the technique of Site-to-site Virtual Private Network (VPN).**

#### **VIRTUAL PRIVATE NETWORK (VPN) PROTOCOLS:**

Some computer network protocols have been specifically used for VPN tunnels. The 3 maximum famous VPN tunnelling protocols indexed under keep to compete with every different for popularity withinside the industry. Those types of protocols are in generally not compatible with each other.

**PPTP:** The full abbreviation for this protocol is Point-To-Point Tunnelling Protocol that constructs a channel and encompasses the packet of data. Point-to-Point connection's protocol is utilized to encrypt the information/data amid the connections. The PPTP is one of the most commonly protocol which is used for VPN protocols for the networks of dial-up. It was initially established by Microsoft and has been in practice since the first release of Windows. In addition to Windows, this protocol also used in Mac and Linux.

**IPSec:** The full abbreviation for this protocol is Internet Protocol Security that is utilized all through an Internet Protocol network to secure the communication of Internet [6]. To give encryption, Internet Protocol Security (IPSec) is frequently joined with other VPN's protocols, yet can likewise be utilized without help from anyone else. This is extensively used by the technique of Site-to-Site VPN's and plenty of iOS applications. In general, two modes of Internet Protocol Security runs are used and those are the mode of transport, and the mode of tunnelling respectively.

**L2TP:** The complete abbreviation for this protocol is Layer 2 Tunnelling Protocol which is mentioned by the protocol of tunnelling regularly matched with the security of another VPN protocols, for example, IPSec to set up a deeply safe for the connection of VPN. The tunnelling protocol of Layer 2 makes a channel among the two joining points of L2TP. Data is encrypted through the protocol of IPSec, and the tunnels communicate securely.

**Secure Sockets Layer (SSL) and Transport Layer Security (TLS):** The protocol of Transport Layer Security and Secure Sockets Layer both make a Virtual Private Network connection wherein the net browser serves and the client's entrance applications is limited instead of the whole organization. Online purchasing gateways are normally the usage of the protocol of TSL and also the protocol of SSL. Internet browsers can without much of a stretch change to SSL as they are inserted with Secure Sockets Layer (SSL) and the protocol of Transport Layer Security (TLS). SSL associations have Hypertext Transfer Protocol Secure (https) withinside the initial of the Uniform Resource Locator (URL) alternatively of Hypertext Transfer Protocol Secure.

**OpenVPN:** For the act like an open-source VPN where OpenVPN broadly utilized for Site-to-Site and Point-to-Point connect improvement. It makes use of a standard of TSL and SSL primarily based totally authentication protocol. OpenVPN allows customers to stable their information the use of sincerely indestructible AES (a systematic algorithm)-256bit key encryption.

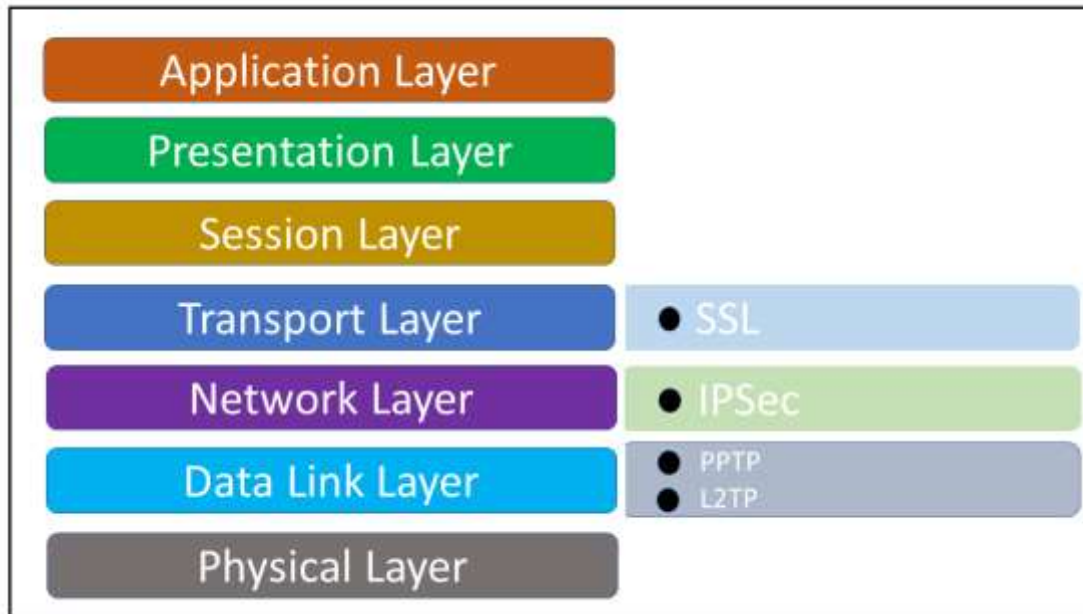


Fig. 7: Presented The protocols of VPN on the model of OSI.

#### FOR THE ISSUES OF SOLVE THE INTERNET SECURITY USING THE TECHNOLOGIES OF VPN:

The milestone technology of Virtual Private Networks uses a variety of tools to defend data flowing through the sector of communication network using internet. Some of the technology utilized by Virtual private networks which has presented in below:

**Firewalls:** Internet firewalls use this type of strategy to check the network address on the port or the packets requested on the arriving connection to determine what traffic is acceptable on the communication of network [10]. Although most of the services of VPN do not directly implement firewalls themselves, they form an essential part of VPNs. The purpose of firewall is to save you undesirable visitors from gaining access to your community at the same time as personal customers of VPN can get admission to it. The filtration of Packet is one of the most common firewalls that stops the intersection of the entry router/switch from determining the address of Internet Protocol. The available example can be presented by the support router of VPN is Cisco-PIX that main aid for filtration of data packet.

**Authentication:** This is a key to the Virtual Private Network's as it ensures the changing events proportion information with the proper Customer or server. It is an identical to "log in" to a username and secret word conspire i.e., the scheme of password. Most of Virtual Private Network authentication is definitely primarily based totally on a public or common key. That keys are controlled with the aid of using the use of an algorithm (i.e., hashing algorithm), generating a cost of hash. The supplementary customer that holds the keys have to create the private of its hash cost and evaluate it to that acquired from the opposite end. The hash esteem shipped off an assailant on the Internet is irrelevant, therefore somebody who sniffs the communication of network would not have the option be capable of accumulate a secret key. The idle example for the system of authentication are CHAP and RSA.

**Encryption:** This is often visible as vital as authentication, as it steady the records being transmitted from the sniffing of packet. Virtual Private Networks utilize 2 normal methods for encryption and those two methods are Hidden (private) and public key respectively, where the encryption of public key calls for a personal and a public key. The user monitors their personal key to all however hold that user's personal key by the user themselves only. Moreover, in secret key encryption, every one of the gatherings that essential to the encoded data have a particular mystery secret key, that is utilized for encrypting just as to decode the data.

## VI. CONCLUSION

VPNs permit customers and businesses to talk on the general sharable net (for example: public internet) to a faraway communication server, sub-office or the commercial enterprise even as keeping steady conversation. VPNs are enormously protected, adaptable, cheaper conversation tool. According to this study, we described numerous Virtual Private Network technology which incorporates Secure Sockets Layer and Internet Protocol Security are famous. Virtual Private Networks can offer the important number of validations, integrity and the procedures of encryption. The future is waiting for a challenging stage for protecting the data, and most of the expert has a higher expectation of getting a strong defence from the technology of Virtual Private Network.



## REFERENCES

- [1]. A. G. Yayimli, "Selective survivability with disjoint nodes and disjoint lightpaths for layer 1 VPN," 2007 First International Symposium on Advanced Networks and Telecommunication Systems, 2007, pp. 1-2, doi: 10.1109/ANTS.2007.4620204.
- [2]. C. A. Augustine, C. O. Anthony, C. O. Maryrose, N. Chukwudi, and I. A. Cosmas, "Analysis of Dynamic Virtual Private Networks Resource Allocation Schemes," International Journal of Communications Network and System Sciences, Vol.11 No.4, 2018, ISSN (P): 1913-3715.
- [3]. M. Ikram, N. V.-Rodriguez, S. Seneviratne, M. A. Kaafar, and V. Paxson, "An Analysis of the Privacy and Security Risks of Android VPN Permission-enabled Apps, Nov. 2016, Pages 349–364,
- [4]. M. Elezi, B. Raufi, "Conception of Virtual Private Networks Using IPsec Suite of Protocols, Comparative Analysis of Distributed Database Queries Using Different IPsec Modes of Encryption, Procedia - Social and Behavioral Sciences," Procedia - Social and Behavioral Sciences, Elsevier, 3 July 2015, Volume 195, Pages 1938-1948, ISSN 1877-0428, <https://doi.org/10.1016/j.sbspro.2015.06.206>.
- [5]. A. A. Jaha, F. B. Shatwan and M. Ashibani, "Proper Virtual Private Network (VPN) Solution," 2008 The Second International Conference on Next Generation Mobile Applications, Services, and Technologies, 2008, pp. 309-314, doi: 10.1109/NGMAST.2008.18.
- [6]. A. V. Uskov, "Information Security of IPsec-based Mobile VPN: Authentication and Encryption Algorithms Performance," 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, 2012, pp. 1042-1048, doi: 10.1109/TrustCom.2012.187.
- [7]. D. Dinkar, P. Greve, K. Landfield, F. Paget, et al., "McAfee Labs Threats Report," 2821 Mission College Boulevard, Santa Clara, CA 95054, March-2016, [Online] Available: <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-quarterly-threats-mar-2016.pdf>
- [8]. "2021 Cyber Security Statistics The Ultimate List Of Stats, Data & Trends," PurpleSec LLC, 2151 Tannin Place, Vienna, Virginia 22182. [Online] Available: <https://purplesec.us/resources/cyber-security-statistics/>
- [9]. A. R. McGee, S. R. Vasireddy, K. J. Johnson, U. Chandrashekhar, S. H. Richman and M. El-Sayed, "Dynamic virtual private networks," in Bell Labs Technical Journal, vol. 6, no. 2, pp. 116-135, 2002, doi: 10.1002/bltj.9.
- [10]. F. Yan, Y. Jian-Wen and C. Lin, "Computer Network Security and Technology Research," 2015 Seventh International Conference on Measuring Technology and Mechatronics Automation, 2015, pp. 293-296, doi: 10.1109/ICMTMA.2015.77.

## BIOGRAPHY



**Md. Zihadul Islam** - He is a final year student of Bangladesh University in B.Sc. of Computer Science and Engineering Department. as well as he is working as an part time IT Officer under Chrom-World Bangladesh Ltd in Dhaka, Bangladesh. In the future he wants to work in communication technology to earn a lot of knowledge about network security.



**Mohammad Arifin Rahman Khan** - Received his Research degree from Edith Cowan University, Australia in 2019 and has completed the M.Sc. degree from London Metropolitan University, London in 2010. As well as, he has made to upgrade his professional career by the specialized certificate CCNA from CISCO. He is also working with the International Journal of Computer Science and Business Informatics (IJCSBI) like an Associate Editor. His research interests include mobility management, multimedia transmission, and quality-of-service (QoS) etc. provision issues in the next-generation of wireless/mobile networks.



**Md. Ibrahim Hossain** - He has completed the Masters in E-Commerce from London, UK. He had completed Bachelor Degree in Computer Science and Engineering from The National Technical University of Ukraine, Kiev, Ukraine. He has successfully completed Cisco Certified Network Associate (CCNA), Microsoft Certified Technology Specialist (MCTS) and Microsoft Certified T Professional (MCITP) on Server 2008 platform. He is also nominated Book Reviewer of The National Curriculum of Textbook Board. His research interest includes Operatig Systems, Networking, and Microwave Technology.



**Rabbi Hossain** - He is the first year student of Bangladesh University in B.Sc. of Computer Science and Engineering Department. In future he wants to work with the field of modern technology and communication.